Subject: Re: Considering different approach to Win32 release
Posted by mirek on Tue, 03 Nov 2015 08:52:17 GMT
View Forum Message <> Reply to Message

mdelfede wrote on Mon, 02 November 2015 18:10
Or, better said, a possible solution would be to leave fixups unencrypted, but then we'd need a table somewhere to tell decrypter to leave them alone. Not an easy task either, and would entail the complete PE header analysis.

Maybe you could limit crypting only to specific opcodes... I believe that only "absolute address" opcodes are 'dangerous'.

You could use ndisasm for testing (although it is a bit disgusting to use opensource to close the source :)

Mirek